

Informazioni su Identity Service Engine (ISE) e Active Directory (AD)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Protocolli AD](#)

[Protocollo Kerberos](#)

[Protocollo MS-RPC](#)

[Integrazione di ISE con Active Directory \(AD\)](#)

[Iscriviti ad ISE 2008](#)

[Aggiungi a dominio Active Directory](#)

[Lascia il dominio Active Directory](#)

[failover DC](#)

[Comunicazione ISE-AD tramite LDAP](#)

[Autenticazione utente in base al flusso AD:](#)

[Filtri di ricerca ISE](#)

Introduzione

In questo documento viene descritto il modo in cui comunicano Identity Service Engine (ISE) e Active Directory (AD), i protocolli utilizzati, i filtri e i flussi di Active Directory.

Prerequisiti

Requisiti

Cisco consiglia una conoscenza di base di:

- Integrazione con ISE 2.x e Active Directory .
- Autenticazione di identità esterna su ISE.

Componenti usati

- ISE 2.x
- Server Windows (Active Directory).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Protocolli AD

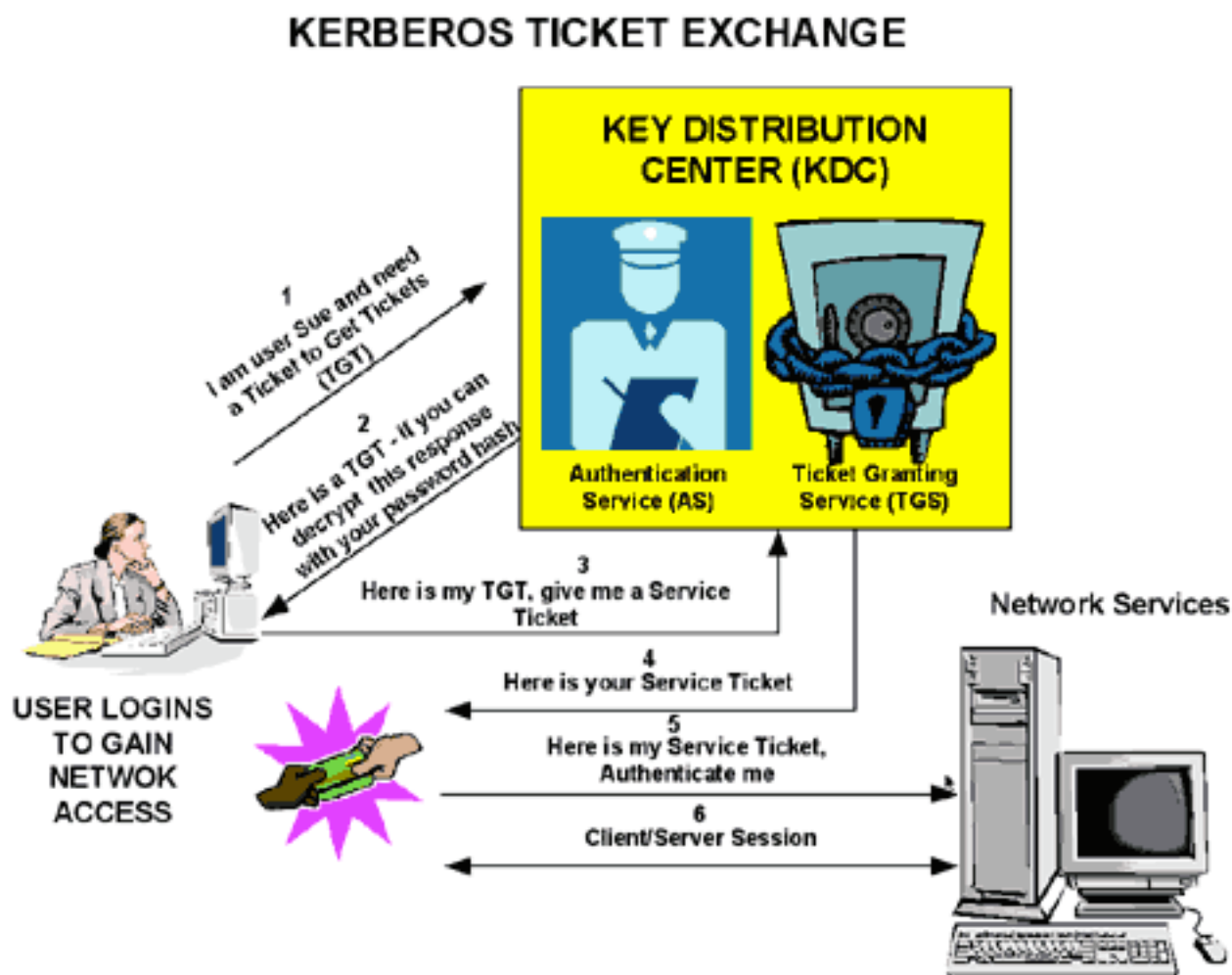
Protocollo Kerberos

I tre capi di Kerberos comprendono il centro distribuzione chiavi (KDC), l'utente client e il server a cui accedere.

Il KDC viene installato come parte del controller di dominio ed esegue due funzioni di servizio: il servizio di autenticazione (AS) e il servizio di concessione ticket (TGS).

Quando il client accede inizialmente a una risorsa server, vengono coinvolti tre scambi:

1. COME Exchange.
2. TGS Exchange.
3. Exchange client/server (CS).



- Controller di dominio = KDC (AS + TGS).

- Autenticare in AS (il portale SSO) con la password.
- Ottenere un ticket di concessione ticket (TGT, Ticket Granting Ticket) (un cookie di sessione).
- Richiedere l'accesso a un servizio (SRV01).
- SRV01 ti reindirizza a KDC.
- Mostra TGT a KDC - (già autenticato)
- KDC offre TGS per SRV01.
- Reindirizzare a SRV01.
- Mostra ticket di servizio per SRV01.
- SRV01 verifica/considera attendibile il ticket di servizio.
- Il ticket di assistenza contiene tutte le mie informazioni.
- SRV01 consente l'accesso.

Quando si accede inizialmente a una rete, gli utenti devono negoziare l'accesso e fornire un nome di accesso e una password per poter essere verificati dalla parte AS di un KDC all'interno del proprio dominio.

Il KDC ha accesso alle informazioni sull'account utente di Active Directory. Una volta autenticato, all'utente viene concesso un ticket TGT valido per il dominio locale.

Il TGT ha una durata predefinita di 10 ore e viene rinnovato per tutta la sessione di accesso dell'utente senza che l'utente debba reimmettere la propria password.

Il TGT viene memorizzato nella cache del computer locale nello spazio di memoria volatile e viene utilizzato per richiedere sessioni con servizi in tutta la rete.

L'utente presenta il TGT alla parte TGS del KDC quando è necessario accedere a un servizio server.

Il TGS sul KDC autentica il TGT utente e crea un ticket e una chiave di sessione sia per il client che per il server remoto. Queste informazioni (il ticket di servizio) vengono quindi memorizzate nella cache locale del computer client.

Il TGS riceve il TGT client e lo legge con la propria chiave. Se il TGS approva la richiesta del client, viene generato un ticket di servizio sia per il client che per il server di destinazione.

Il client legge la propria parte con la chiave di sessione TGS recuperata in precedenza dalla risposta AS.

Il client presenta la parte server della risposta TGS al server di destinazione nel successivo scambio client/server.

Esempio:

Test User Authentication

* Username

* Password

Authentication Type

Authorization Data Retrieve Groups
 Retrieve Attributes

Authentication Result	Groups	Attributes
<pre> Authentication time : 57 ms. Groups fetching time : 18 ms. Attributes fetching time: 4 ms. Processing Steps: 14:05:37:440: Resolving identity - user1 14:05:37:440: Search for matching accounts at join point - ralmaait.com 14:05:37:449: Single matching account found in forest - ralmaait.com 14:05:37:449: Identity resolution detected single matching account 14:05:37:476: Authentication Ticket (TGT) request succeeded - user1@ralmaait.com 14:05:37:478: Service Ticket request succeeded - user1@ralmaait.com 14:05:37:486: Service Ticket validation succeeded - user1@ralmaait.com 14:05:37:486: Account validation succeeded </pre>		

Pacchetti acquisiti da ISE per un utente autenticato:

111	2020-01-13 16:17:53.082713	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=105462807 TSecr=280789807 ✓
112	2020-01-13 16:17:53.082735	10.48.60.50	10.48.60.51	KRB5	346 AS-REQ ✓
113	2020-01-13 16:17:53.083625	10.48.60.51	10.48.60.50	KRB5	1576 AS-REP ✓
114	2020-01-13 16:17:53.083649	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [ACK] Seq=281 Ack=1511 Win=32256 Len=0 TSval=105462808 TSecr=2807... ✓
115	2020-01-13 16:17:53.083678	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [FIN, ACK] Seq=281 Ack=1511 Win=32256 Len=0 TSval=105462808 TSecr=2807... ✓
116	2020-01-13 16:17:53.083908	10.48.60.51	10.48.60.50	TCP	66 88 → 53610 [ACK] Seq=1511 Ack=282 Win=532736 Len=0 TSval=280789809 TSecr=105... ✓
117	2020-01-13 16:17:53.084022	10.48.60.51	10.48.60.50	TCP	60 88 → 53610 [RST, ACK] Seq=1511 Ack=282 Win=0 Len=0 ✓
118	2020-01-13 16:17:53.084449	10.48.60.50	10.48.60.51	KRB5	1480 TGS-REQ ✓
119	2020-01-13 16:17:53.085475	10.48.60.51	10.48.60.50	KRB5	1446 TGS-REP ✓
120	2020-01-13 16:17:53.110397	10.48.60.50	10.48.60.51	TCP	66 48959 → 3268 [ACK] Seq=1700 Ack=536 Win=31360 Len=0 TSval=105462835 TSecr=28... ✓

AS-REQ contiene il nome utente. Se la password è corretta, il servizio AS fornisce un TGT crittografato con la password utente. Il TGT viene quindi fornito al servizio TGT per ottenere un ticket di sessione.

L'autenticazione ha esito positivo alla ricezione di un ticket di sessione.

Questo è un esempio di password errata fornita dal client:

117	2020-01-14 08:51:03.846603	10.48.60.50	10.48.60.51	KRB5	318 AS-REQ
118	2020-01-14 08:51:03.848340	10.48.60.51	10.48.60.50	KRB5	194 KRB Error: KRB5KDC_ERR_PREAUTH_FAILED

Se la password è errata, la richiesta AS ha esito negativo e non viene ricevuto un TGT:

Processing Steps:	
13:19:55:837:	Resolving Identity - User1
13:19:55:837:	Search For Matching Accounts At Join Point - Ralmaait.com
13:19:55:843:	Single Matching Account Found In Forest - Ralmaait.com
13:19:55:843:	Identity Resolution Detected Single Matching Account
13:19:55:856:	Authentication Ticket (TGT) Request Failed - User1@ralmaait.com, ERROR_PASSWORD_MISMATCH

Esegue l'accesso al file ad_agent.log quando la password è errata:

2020-01-14 13:36:05,442 DEBUG ,140574072981248,krb5: Inviata richiesta (276 byte) a RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG ,140574072981248,krb5: Errore ricevuto da KDC: -1765328360/Preautenticazione non riuscita,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG ,140574072981248,krb5: Riprovare prima Tipi di input: 16, 14, 19, 2,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 WARNING,140574072981248,[LwKrb5GetTgtImpl ../lwadvapi/threaded/krbtgt.c:329] KRB5 Codice di errore: -1765328360 (Messaggio: Preautenticazione non riuscita),LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

2020-01-14 13:36:05,444 DEBUG ,140574072981248,[LwKrb5InitializeUserLoginCredentials()] Codice di errore: 40022 (simbolo: LW_ERROR_PASSWORD_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwkrb5.c:1325

Protocollo MS-RPC

ISE utilizza MS-RPC su SMB, SMB fornisce l'autenticazione e non richiede una sessione separata per individuare la posizione di un determinato servizio RPC. Utilizza un meccanismo denominato "named pipe" per comunicare tra il client e il server.

- Creare una connessione di sessione SMB.
- Trasporta messaggi RPC su SMB/CIFS.TCP porta 445 come trasporto
- La sessione SMB identifica la porta utilizzata da un determinato servizio RPC e gestisce l'autenticazione utente.
- Connettersi alla condivisione nascosta IPC\$ per la comunicazione tra processi.
- Aprire una named pipe appropriata per la funzione o la risorsa RPC desiderata.

Transazione dello scambio RPC su SMB.

No.	Time	Source	Destination	Protocol	Length	Info	Text Item
59	2020-01-14 14:56:01.082699	10.48.60.50	10.48.60.51	SMB	128	Negotiate Protocol Request	✓
60	2020-01-14 14:56:01.083241	10.48.60.51	10.48.60.50	SMB2	318	Negotiate Protocol Response	✓
61	2020-01-14 14:56:01.083255	10.48.60.50	10.48.60.51	TCP	66	26963 → 445 [ACK] Seq=63 Ack=253 Win=30336 Len=0 TSval=186958007 TSecr=36222...	✓
72	2020-01-14 14:56:01.086109	10.48.60.50	10.48.60.51	SMB2	1509	Session Setup Request	✓
73	2020-01-14 14:56:01.086341	10.48.60.51	10.48.60.50	TCP	66	445 → 26963 [ACK] Seq=253 Ack=1586 Win=66560 Len=0 TSval=362277347 TSecr=186...	✓
74	2020-01-14 14:56:01.087051	10.48.60.51	10.48.60.50	SMB2	328	Session Setup Response	✓
75	2020-01-14 14:56:01.087260	10.48.60.50	10.48.60.51	SMB2	212	Tree Connect Request Tree: \\WIN-E051AB1Q9BK.raismait.com\IPC\$	✓
76	2020-01-14 14:56:01.087592	10.48.60.51	10.48.60.50	SMB2	150	Tree Connect Response	✓
77	2020-01-14 14:56:01.087721	10.48.60.50	10.48.60.51	SMB2	206	Create Request File: netlogon	✓
78	2020-01-14 14:56:01.088023	10.48.60.51	10.48.60.50	SMB2	222	Create Response File: netlogon	✓
79	2020-01-14 14:56:01.088207	10.48.60.50	10.48.60.51	DCERPC	314	Bind: call_id: 9, Fragment: Single, 1 context items: RPC_NETLOGON V1.0 (32bi...	✓
80	2020-01-14 14:56:01.088500	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓
81	2020-01-14 14:56:01.088665	10.48.60.50	10.48.60.51	SMB2	183	Read Request Len:8192 Off:0 File: netlogon	✓
82	2020-01-14 14:56:01.088899	10.48.60.51	10.48.60.50	DCERPC	238	Bind ack: call_id: 9, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 res...	✓
83	2020-01-14 14:56:01.089118	10.48.60.50	10.48.60.51	RPC_NETLOGON	574	NetLogonSamLogonEx request	✓
84	2020-01-14 14:56:01.089373	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓
85	2020-01-14 14:56:01.089517	10.48.60.50	10.48.60.51	SMB2	183	Read Request Len:8192 Off:0 File: netlogon	✓
86	2020-01-14 14:56:01.090160	10.48.60.51	10.48.60.50	RPC_NETLOGON	606	NetLogonSamLogonEx response	✓
88	2020-01-14 14:56:01.129364	10.48.60.50	10.48.60.51	TCP	66	26963 → 445 [ACK] Seq=2862 Ack=1635 Win=34688 Len=0 TSval=186958054 TSecr=36...	✓
145	2020-01-14 14:56:09.918387	10.48.60.50	10.48.60.51	RPC_NETLOGON	574	NetLogonSamLogonEx request	✓
146	2020-01-14 14:56:09.918734	10.48.60.51	10.48.60.50	CHR2	150	Write Response	✓

```

> Secure Channel Verifier
Microsoft Network Logon, NetLogonSamLogonEx
Operation: NetLogonSamLogonEx (39)
[Response in frame: 86]
LogonServer: \\WIN-E051AB1Q9BK.raismait.com
Referent ID: 0x00000001
Max Count: 31
Offset: 0
Actual Count: 31
Computer Name: \\WIN-E051AB1Q9BK.raismait.com
Computer Name: ISERIR124
Referent ID: 0x00000001
Max Count: 10
Offset: 0
Actual Count: 10
Computer Name: ISERIR124
Level: 2
LEVEL: LogonLevel
Level: 2
NETWORK_INFO:
Referent ID: 0x00000001
IDENTITY_INFO: user1@raismait.com
Challenge: cdc343b187f9b4e1

```

OSPF (Open Shortest Path First) negotiate protocol request/response La linea negozia il dialetto di SMB.
 OSPF (Open Shortest Path First) session setup request/response esegue l'autenticazione.

La richiesta e la risposta di connessione alla struttura si connettono alla risorsa richiesta. Si è connessi a una condivisione speciale IPC\$.

Questa condivisione di comunicazione tra processi fornisce i mezzi di comunicazione tra gli host e anche come trasporto per le funzioni MSRPC.

Al pacchetto 77 è Create Request File e il nome file è il nome del servizio connesso (il servizio netlogon in questo esempio).

Ai pacchetti 83 e 86, la richiesta NetlogonSamLogonEX è dove si invia il nome utente per l'autenticazione del client su ISE all'AD sul campo Network_INFO.

Il pacchetto di risposta NetlogonSamLogonEX risponde con i risultati.

Alcuni valori dei flag per la risposta NetlogonSamLogonEX:

0xc00006a è STATUS_WRONG_PASSWORD

0x00000000 è STATUS_SUCCESS

0x0000103 è STATUS_PENDING

Integrazione di ISE con Active Directory (AD)

ISE utilizza LDAP, KRB e MSRBC per comunicare con AD durante il processo di unione/uscita e

autenticazione.

Nelle sezioni seguenti vengono illustrati i protocolli, il formato di ricerca e i meccanismi utilizzati per connettersi a un controller di dominio specifico in Active Directory e per l'autenticazione degli utenti in base a tale controller di dominio.

Nel caso in cui il controller di dominio diventi offline per qualsiasi motivo, ISE esegue il failover sul successivo controller di dominio disponibile e il processo di autenticazione non subisce modifiche.

Un server di catalogo globale è un controller di dominio in cui vengono archiviate copie di tutti gli oggetti Active Directory della foresta.

Memorizza una copia completa di tutti gli oggetti nella directory del dominio e una copia parziale di tutti gli oggetti di tutti gli altri domini della foresta.

Pertanto, il catalogo globale consente agli utenti e alle applicazioni di trovare oggetti in qualsiasi dominio della foresta corrente con una ricerca di attributi inclusi nel catalogo globale.

Il catalogo globale contiene un set di attributi di base (ma incompleto) per ogni oggetto foresta in ogni dominio (Set di attributi parziali, PAT).

Il catalogo globale riceve i dati da tutte le partizioni di directory di dominio nella foresta. Vengono copiati con il servizio di replica standard di Active Directory.

Iscriviti ad ISE 2008

Prerequisiti per l'integrazione con Active Directory e ISE

1. Verificare di disporre dei privilegi di amministratore privilegiato o di amministratore di sistema in ISE.
2. Utilizzare le impostazioni del server NTP (Network Time Protocol) per sincronizzare l'ora tra il server Cisco e Active Directory. La differenza massima consentita tra ISE e AD è di 5 minuti
3. Il DNS configurato su ISE deve essere in grado di rispondere alle query SRV per DC, GC e KDC con o senza ulteriori informazioni sul sito.
4. Verificare che tutti i server DNS siano in grado di rispondere alle query DNS di inoltro e di inversione per qualsiasi possibile dominio DNS di Active Directory.
5. Ad deve disporre di almeno un server di catalogo globale operativo e accessibile da Cisco, nel dominio a cui si accede a Cisco.

Aggiungi a dominio Active Directory

ISE applica la funzionalità di individuazione del dominio per ottenere informazioni sul dominio di join in tre fasi:

1. Interroga i domini uniti: individua i domini della relativa foresta e i domini trusted esternamente al dominio aggiunto.
2. Interroga i domini radice nella relativa foresta - Stabilisce il trust con la foresta.


3. Interroga i domini radice nelle foreste trusted: individua i domini dalle foreste trusted.

Cisco ISE individua inoltre i nomi di dominio DNS (suffissi UPN), i suffissi UPN alternativi e i nomi di dominio NTLM.

ISE applica un'individuazione CC per ottenere tutte le informazioni sui controller di dominio e i cataloghi disponibili.

1. Il processo di aggiunta inizia con le credenziali di input di amministratore privilegiato in Active Directory presenti nel dominio stesso. Se esiste in un dominio o un sottodominio diverso, il nome utente deve essere indicato in una notazione UPN (username@domain).
2. ISE invia una query DNS per tutti i record di controller di dominio, cataloghi globali e KDC. Se la risposta DNS non conteneva una di queste risposte, l'integrazione non riesce con un errore correlato al DNS.
3. ISE utilizza il ping CLDAP per individuare tutti i controller di dominio e i cataloghi tramite le richieste CLDAP inviate ai controller di dominio che corrispondono alle relative priorità nel record SRV. si utilizza la prima risposta del CC e l'ISE viene collegata a quel CC.

Un fattore utilizzato per calcolare la priorità del controller di dominio è il tempo impiegato dal controller di dominio per rispondere ai ping CLDAP. Una risposta più rapida riceve una priorità più alta.

 Nota: CLDAP è il meccanismo utilizzato da ISE per stabilire e mantenere la connettività con i controller di dominio. Misura il tempo di risposta fino alla prima risposta DC. Non funziona se non si vede alcuna risposta da DC. Avvisa se il tempo di risposta è superiore a 2,5 secondi. CLDAP esegue il ping di tutti i controller di dominio nel sito (se non è presente alcun sito, verranno eseguiti tutti i controller di dominio nel dominio). La risposta CLDAP contiene il sito DC e il sito client (il sito a cui è assegnata la macchina ISE).

4. ISE riceve quindi il TGT con le credenziali di "join user".
5. Generare il nome dell'account del computer ISE con MSRPC (SAM e SPN).
6. Se l'account del computer ISE esiste già, eseguire una ricerca in Active Directory in base all'SPN. Se ISE non esiste, ne viene creato uno nuovo.
7. Aprire l'account del computer, impostare la password dell'account del computer ISE e verificare che l'account del computer ISE sia accessibile.
8. Impostare gli attributi dell'account del computer ISE (SPN, dnsHostname e simili).
9. Ottieni TGT con le credenziali del computer ISE con KRB5 e scopri tutti i domini trusted.
10. Una volta completato il join, il nodo ISE aggiorna i gruppi AD e i SID associati e avvia automaticamente il processo di aggiornamento del SID. Verificare che il processo possa essere completato sul lato AD.

Lascia il dominio Active Directory

Quando ISE esce, l'AD deve considerare:

1. Utilizzare un utente amministratore AD completo per eseguire i processi di uscita. In questo modo si verifica che l'account del computer ISE venga rimosso dal database di Active

Directory.

2. Se AD è stato lasciato senza credenziali, l'account ISE non viene rimosso da AD e deve essere eliminato manualmente.
3. Quando si ripristina la configurazione ISE dalla CLI o si ripristina la configurazione dopo un backup o un aggiornamento, viene eseguita un'operazione di uscita e il nodo ISE viene disconnesso dal dominio Active Directory. (se unito). Tuttavia, l'account del nodo ISE non viene rimosso dal dominio Active Directory.
4. È consigliabile eseguire un'operazione di uscita dal portale di amministrazione con le credenziali di Active Directory, in quanto l'account del nodo viene rimosso anche dal dominio di Active Directory. Questa opzione è consigliata anche quando si modifica il nome host ISE.

failover DC

Quando il DC connesso all'ISE diventa offline o irraggiungibile per qualsiasi motivo, il failover del DC viene attivato automaticamente sull'ISE. Il failover del controller di dominio può essere attivato dalle seguenti condizioni:

1. Il connettore AD rileva che il controller di dominio attualmente selezionato non è più disponibile durante alcuni tentativi di comunicazione CLDAP, LDAP, RPC o Kerberos. In questi casi, il connettore AD avvia la selezione del controller di dominio e ne esegue il failover nel controller di dominio appena selezionato.
2. Il controller di dominio è attivo e risponde al ping CLDAP, ma il connettore AD non è in grado di comunicare con esso per qualche motivo (ad esempio, la porta RPC è bloccata, il controller di dominio è in stato di 'replica interrotta', le autorizzazioni per il controller di dominio non sono state rimosse correttamente).

In questi casi, il connettore AD avvia la selezione del controller di dominio con un elenco bloccato (il controller di dominio "danneggiato" viene inserito nell'elenco bloccato) e tenta di comunicare con il controller di dominio selezionato. Il controller di dominio selezionato nell'elenco dei controller di dominio bloccati non è memorizzato nella cache.

Il connettore AD deve completare il failover entro un tempo ragionevole (o interromperlo se non è possibile). Per questo motivo, il connettore AD tenta di utilizzare un numero limitato di controller di dominio durante il failover.

ISE blocca i controller di dominio Active Directory in caso di errore irreversibile della rete o del server per impedire ad ISE di utilizzare un controller di dominio danneggiato. Il controller di dominio non viene aggiunto all'elenco dei controller bloccati se non risponde ai ping CLDAP. L'ISE riduce solo la priorità del controller di dominio che non risponde.

Comunicazione ISE-AD tramite LDAP

ISE esegue la ricerca di computer o utenti in Active Directory in uno dei seguenti formati di ricerca. Se la ricerca riguardava un computer, ISE aggiunge "\$" alla fine del nome del computer. Elenco di tipi di identità utilizzati per identificare un utente in Active Directory:

- Nome SAM: nome utente o nome computer senza markup di dominio. Si tratta del nome di

accesso utente in Active Directory. Esempio: sajeda o sajeda\$

- CN: è il nome visualizzato dell'utente in AD. Non deve essere uguale al SAM. Esempio: sajeda Ahmed.
- Nome dell'entità utente (UPN): è una combinazione del nome SAM e del nome di dominio (SAM_NAME@domian). Esempio: sajeda@cisco.com o sajeda\$@cisco.com
- UPN alternativo: è un suffisso UPN aggiuntivo/alternativo configurato in Active Directory diverso dal nome di dominio. Questa configurazione viene aggiunta globalmente in Active Directory (non configurata per utente) e non è necessario che sia un suffisso di nome di dominio reale.

Ogni AD può avere più suffissi UPN (@alt1.com,@alt2.com,..., ecc.). Esempio: UPN principale (sajeda@cisco.com), UPN alternativo:sajeda@domain1 , sajeda@domain2

- Nome prefisso NetBIOS: è il nome di dominio omeutente del nome del computer. Esempio: CISCO\sajeda o CISCO\machine\$
- Host/prefisso con computer non qualificato: viene utilizzato per l'autenticazione del computer quando viene utilizzato solo il nome del computer, è solo il nome dell'host/computer. Esempio: host/computer
- Host/prefisso con computer completo: utilizzato per l'autenticazione del computer quando viene utilizzato il nome di dominio completo (FQDN) del computer, in genere nel caso dell'autenticazione del certificato, è host/FQDN del computer. Esempio: host/machine.cisco.com
- Nome SPN: il nome con cui un client identifica in modo univoco un'istanza di un servizio (esempi: HTTP, LDAP, SSH) utilizzato solo per il computer.

Autenticazione utente in base al flusso AD:

1. Risolvere l'identità e determinare il tipo di identità: SAM, UPN, SPN. Se ISE riceve l'identità solo come nome utente, cerca un account SAM associato in Active Directory. Se ISE riceve l'identità come username@domain, cerca un UPN o un indirizzo di posta corrispondente nell'AD. in entrambi gli scenari ISE utilizza filtri aggiuntivi per il computer o il nome utente.
2. Cerca nel dominio o nella foresta (dipende dal tipo di identità)
3. Mantieni informazioni su tutti gli account associati (JP, DN, UPN, Dominio)
4. Se non viene trovato alcun account associato, AD risponde con l'utente sconosciuto.
5. Esegui autenticazione MS-RPC (o Kerberos) per ogni account associato
6. Se solo un account corrisponde all'identità e alla password di input, l'autenticazione avrà esito positivo
7. Se più account corrispondono all'identità in ingresso, ISE utilizza la password per risolvere l'ambiguità in modo che l'account con una password associata venga autenticato e gli altri account aumentino di 1 il contatore della password errato.
8. Se nessun account corrisponde all'identità e alla password in ingresso, AD risponde con una password errata.

ISE Filtri di ricerca

I filtri vengono utilizzati per identificare un'entità che desidera comunicare con AD. ISE cerca sempre tale entità nei gruppi utenti e computer.

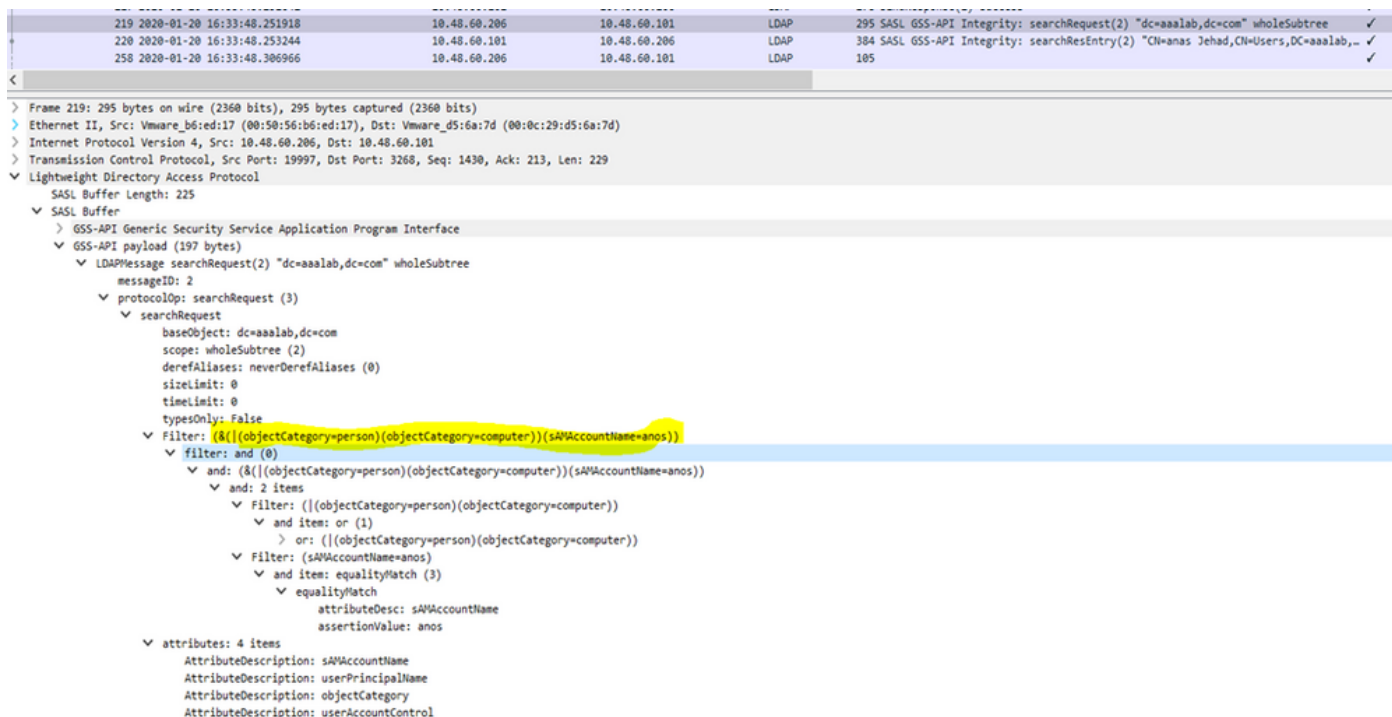
Esempi di filtri di ricerca:

1. Ricerca SAM: se ISE riceve un'identità come solo nome utente senza alcun markup di dominio, considera questo nome utente come SAM e cerca in AD tutti i computer, utenti o computer che hanno quell'identità come nome SAM.

Se il nome SAM non è univoco, ISE utilizza la password per distinguere gli utenti e ISE è configurato per utilizzare un protocollo senza password, ad esempio EAP-TLS.

Non esistono altri criteri per individuare l'utente giusto, quindi ISE non riesce l'autenticazione con un errore di "Identità ambigua".

Tuttavia, se il certificato utente è presente in Active Directory, Cisco ISE utilizzerà il confronto binario per risolvere l'identità.



```
> 219 2020-01-20 16:33:48.251918 10.48.60.206 10.48.60.101 LDAP 295 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree ✓
> 220 2020-01-20 16:33:48.253244 10.48.60.101 10.48.60.206 LDAP 384 SASL GSS-API Integrity: searchResEntry(2) "CN=anas Jehad,CN=Users,DC=aaalab,DC=com" ✓
> 258 2020-01-20 16:33:48.306966 10.48.60.206 10.48.60.101 LDAP 185 ✓

<
> Frame 219: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface 0
> Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
> Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
> Transmission Control Protocol, Src Port: 19997, Dst Port: 3268, Seq: 1430, Ack: 213, Len: 229
> Lightweight Directory Access Protocol
  SASL Buffer Length: 225
  SASL Buffer
  > GSS-API Generic Security Service Application Program Interface
  > GSS-API payload (197 bytes)
  > LDAPMessage searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
    messageID: 2
    > protocolOp: searchRequest (3)
      > searchRequest
        baseObject: dc=aaalab,dc=com
        scope: wholeSubtree (2)
        derefAliases: neverDerefAliases (0)
        sizeLimit: 0
        timeLimit: 0
        typesOnly: False
        > Filter: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
          > filter: and (0)
            > and: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
              > and: 2 items
                > Filter: ((objectCategory=person)(objectCategory=computer))
                  > and item: or (1)
                    > or: ((objectCategory=person)(objectCategory=computer))
                      > Filter: (sAMAccountName=anos)
                        > and item: equalityMatch (3)
                          > equalityMatch
                            attributeDesc: sAMAccountName
                            assertionValue: anos
              > attributes: 4 items
                AttributeDescription: sAMAccountName
                AttributeDescription: userPrincipalName
                AttributeDescription: objectCategory
                AttributeDescription: userAccountControl
```

2. Ricerca per UPN o per posta: se ISE riceve un'identità come username@domain, cerca in ogni catalogo globale della foresta una corrispondenza con l'identità UPN o con l'identità di posta "identity=upn o email corrispondente".

Se esiste una corrispondenza unica, Cisco ISE procede con il flusso AAA.

Se sono presenti più punti di join con lo stesso UPN e la stessa password o con lo stesso UPN e la stessa posta, Cisco ISE non riesce a eseguire l'autenticazione con un errore di "identità ambigua".

461	2020-01-20 16:33:58.134338	10.48.60.206	10.48.60.101	LDAP	336 SASL GSS-API Integrity: searchRequest(3) "dc=aaalab,dc=com" wholeSubtree	✓
464	2020-01-20 16:33:58.137942	10.48.60.101	10.48.60.206	LDAP	384 SASL GSS-API Integrity: searchResEntry(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
471	2020-01-20 16:33:58.170678	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(6) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
472	2020-01-20 16:33:58.172663	10.48.60.101	10.48.60.206	LDAP	1413 SASL GSS-API Integrity: searchResEntry(6) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
476	2020-01-20 16:33:58.174754	10.48.60.206	10.48.60.101	LDAP	189 SASL GSS-API Integrity: searchRequest(7) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
479	2020-01-20 16:33:58.175528	10.48.60.101	10.48.60.206	LDAP	255 SASL GSS-API Integrity: searchResEntry(7) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
480	2020-01-20 16:33:58.176236	10.48.60.206	10.48.60.101	LDAP	241 SASL GSS-API Integrity: searchRequest(8) "dc=aaalab,dc=com" wholeSubtree	✓
481	2020-01-20 16:33:58.177307	10.48.60.101	10.48.60.206	LDAP	635 SASL GSS-API Integrity: searchResEntry(8) "CN=Users,CN=Builtin,DC=aaalab,DC=	✓
484	2020-01-20 16:33:58.178414	10.48.60.206	10.48.60.101	LDAP	271 SASL GSS-API Integrity: searchRequest(9) "dc=aaalab,dc=com" wholeSubtree	✓

```

> Frame 461: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)
> Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
> Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
> Transmission Control Protocol, Src Port: 19997, Dst Port: 3268, Seq: 1659, Ack: 531, Len: 270
> Lightweight Directory Access Protocol
  SASL Buffer Length: 266
  SASL Buffer
    GSS-API Generic Security Service Application Program Interface
    GSS-API payload (238 bytes)
      LDAPMessage searchRequest(3) "dc=aaalab,dc=com" wholeSubtree
        messageID: 3
        protocolOp: searchRequest (3)
          searchRequest
            baseObject: dc=aaalab,dc=com
            scope: wholeSubtree (2)
            derefAliases: neverDerefAliases (0)
            sizeLimit: 0
            timeLimit: 0
            typesOnly: False
            Filter: (&((objectCategory=person)(objectCategory=computer))((userPrincipalName=anas@aaalab.com)(mail=anos@aaalab.com)))
              filter: and (0)
                and: (&((objectCategory=person)(objectCategory=computer))((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com)))
                  and: 2 items
                    Filter: ((objectCategory=person)(objectCategory=computer))
                      and item: or (1)
                        or: ((objectCategory=person)(objectCategory=computer))
                    Filter: ((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com))
                      and item: or (1)
                        or: ((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com))

```

3. Ricerca NetBIOS: se ISE riceve un'identità con un prefisso di dominio NetBIOS (ad esempio, CISCO\sajedah), cerca il dominio NetBIOS nelle foreste. Una volta trovato, cerca il nome SAM fornito (sajeda nell'esempio)

554	2020-01-20 17:06:29.243747	10.48.60.206	10.48.60.101	LDAP	295 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree	✓
555	2020-01-20 17:06:29.245154	10.48.60.101	10.48.60.206	LDAP	682 SASL GSS-API Integrity: searchResEntry(2) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
684	2020-01-20 17:06:29.290383	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
685	2020-01-20 17:06:29.292939	10.48.60.101	10.48.60.206	LDAP	1413 SASL GSS-API Integrity: searchResEntry(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
687	2020-01-20 17:06:29.294515	10.48.60.206	10.48.60.101	LDAP	189 SASL GSS-API Integrity: searchRequest(4) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
688	2020-01-20 17:06:29.295469	10.48.60.101	10.48.60.206	LDAP	255 SASL GSS-API Integrity: searchResEntry(4) "CN=anas Jehad,CN=Users,DC=aaalab,DC=	✓
689	2020-01-20 17:06:29.296186	10.48.60.206	10.48.60.101	LDAP	241 SASL GSS-API Integrity: searchRequest(5) "dc=aaalab,dc=com" wholeSubtree	✓
692	2020-01-20 17:06:29.297557	10.48.60.101	10.48.60.206	LDAP	635 SASL GSS-API Integrity: searchResEntry(5) "CN=Users,CN=Builtin,DC=aaalab,DC=	✓
693	2020-01-20 17:06:29.298761	10.48.60.206	10.48.60.101	LDAP	271 SASL GSS-API Integrity: searchRequest(6) "dc=aaalab,dc=com" wholeSubtree	✓
694	2020-01-20 17:06:29.299698	10.48.60.101	10.48.60.206	LDAP	650 SASL GSS-API Integrity: searchResEntry(6) "CN=Domain Users,CN=Users,DC=aaala-	✓

```

> SASL Buffer
  GSS-API Generic Security Service Application Program Interface
  GSS-API payload (197 bytes)
    LDAPMessage searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
      messageID: 2
      protocolOp: searchRequest (3)
        searchRequest
          baseObject: dc=aaalab,dc=com
          scope: wholeSubtree (2)
          derefAliases: neverDerefAliases (0)
          sizeLimit: 0
          timeLimit: 0
          typesOnly: False
          Filter: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
            filter: and (0)
              and: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
                and: 2 items
                  Filter: ((objectCategory=person)(objectCategory=computer))
                    and item: or (1)
                      or: ((objectCategory=person)(objectCategory=computer))
                  Filter: (sAMAccountName=anos)
                    and item: equalityMatch (3)
                      equalityMatch

```

4. Ricerca per base su computer: se ISE riceve l'autenticazione di un computer, con identità host/prefisso, cerca nella foresta un attributo servicePrincipalName corrispondente.

Se nell'identità è stato specificato un suffisso di dominio completo, ad esempio host/machine.domain.com, Cisco ISE eseguirà una ricerca nella foresta in cui è presente il dominio.

Se l'identità è nel formato host/computer, Cisco ISE cerca il nome dell'entità servizio in tutte le foreste.

In caso di più corrispondenze, Cisco ISE non riesce l'autenticazione con un errore di "Identità ambigua".

2744	2020-01-20	16:35:32.108609	10.48.60.206	10.48.60.101	LDAP	373 SASL GSS-API Integrity: searchRequest(3) "dc=aaalab,dc=com" wholeSubtree	✓
2745	2020-01-20	16:35:32.109744	10.48.60.101	10.48.60.206	LDAP	393 SASL GSS-API Integrity: searchResEntry(3) "CN=ISE24P,CN=Computers,DC=aaalab,DC=aaalab,DC=com" wholeSubtree	✓
2747	2020-01-20	16:35:32.109951	10.48.60.206	10.48.60.101	LDAP	185 SASL GSS-API Integrity: unbindRequest(7)	✓
2757	2020-01-20	16:35:32.114862	10.48.60.206	10.48.60.101	LDAP	1495 bindRequest(1) "<ROOT>" sasl	✓
2758	2020-01-20	16:35:32.115898	10.48.60.101	10.48.60.206	LDAP	278 bindResponse(1) success	✓
2760	2020-01-20	16:35:32.116176	10.48.60.206	10.48.60.101	LDAP	348 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree	✓
2761	2020-01-20	16:35:32.116855	10.48.60.101	10.48.60.206	LDAP	740 SASL GSS-API Integrity: searchResEntry(2) "CN=ISE24P,CN=Computers,DC=aaalab,DC=aaalab,DC=com" wholeSubtree	✓
2762	2020-01-20	16:35:32.145535	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(3) "CN=ISE24P,CN=Computers,DC=aaalab,DC=aaalab,DC=com" wholeSubtree	✓

Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)

Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101

Transmission Control Protocol, Src Port: 28889, Dst Port: 3268, Seq: 1746, Ack: 267, Len: 307

Lightweight Directory Access Protocol

SASL Buffer Length: 303

▼ SASL Buffer

> GSS-API Generic Security Service Application Program Interface

▼ GSS-API payload (275 bytes)

▼ LDAPMessage searchRequest(3) "dc=aaalab,dc=com" wholeSubtree

messageID: 3

▼ protocolOp: searchRequest(3)

▼ searchRequest

baseObject: dc=aaalab,dc=com

scope: wholeSubtree (2)

dereferAliases: neverDereferAliases (0)

sizeLimit: 0

timeLimit: 0

typesOnly: False

▼ Filter: (&(|(objectCategory=person)(objectCategory=computer)))(sAMAccountName=ise24p\$)

▼ filter: and (0)

▼ and: (&(|(objectCategory=person)(objectCategory=computer)))(sAMAccountName=ise24p\$)

▼ and: 2 items

▼ Filter: (|(objectCategory=person)(objectCategory=computer))

▼ and item: or (1)

> or: (|(objectCategory=person)(objectCategory=computer))

▼ Filter: (sAMAccountName=ise24p\$)

▼ and item: equalityMatch (3)

▼ equalityMatch

attributeDesc: sAMAccountName

assertionValue: ise24p\$



Nota: gli stessi filtri si trovano nei file ad-agent.log di ISE



Nota: ISE 2.2 patch 4 e precedenti e 2.3 patch 1 e gli utenti precedentemente identificati con gli attributi SAM, CN o entrambi. Cisco ISE, release 2.2 Patch 5 e successive, e 2.3 Patch 2 e successive, utilizzano solo l'attributo sAMAccountName come attributo predefinito.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).